REMARKS:

In the outstanding Office Action, the Examiner rejected claims 1-4, 6-24 and 26-41. Claims 1, 20, 21, 40 and 41 are amended herein. No new matter is presented. Claims 5 and 25 remain cancelled. Thus, claims 1-4, 6-24 and 26-41 are pending and under consideration. The rejections are traversed below.

CLAIM REJECTIONS UNDER 35 USC §102:

In the Office Action the Examiner rejected claims 1-4, 6-24 and 26-41 under 35 U.S.C. §102(b) as being anticipated by U.S. Patent No. 5,987,557(Ebrahim). The Applicants respectfully traverse the Examiner's rejections of the remaining claims.

Claim 1, by way of example, recites "... **a tamper resistant module structure inaccessible from outside** that stores information related to secure software" and "a falsification checking unit... [that] **reads the secure software from the memory by direct access without using the operating system**, compares the read secure software...and checks..." (emphasis added). The Applicants respectfully submit that Ebrahim does not disclose or suggest at least this feature of claim 1. See also other independent claims reciting similar features.

Ebrahim discusses a protection check circuit configured at initialization time by an operating system or a privileged software process for monitoring transactions on the data paths. However, Ebrahim is limited to generating an allowability signal based on comparison of transaction path signals and signals in the storage designating the protection domains (see, column 7, lines 2-16).

Ebrahim explicitly states:

> "a system controller block112, and
>
> the protection check logic connected to the access control path for snooping on transactions on the transaction path...includes a storage connected to the protection check logic...the storage stores transaction allowability data...includes a decision logic compares transaction data on the transaction path to transaction allowability data."

(see, Fig.1, column 3, lines 29 to 45 of Ebrahim).

As described above, Ebrahim merely discusses a system controller block and a protection check logic that stores transaction allowability data and compares a transaction data on the transaction path to the transaction allowability data to implement hardware protection.

It is respectfully submitted that Ebrahim does not discuss, teach or suggest a hardware secure module having "a tamper resistant module structure inaccessible from outside that stores information related to secure software" and "a falsification checking unit that reads the secure software from the memory by direct access without using the operating system, compares the read secure software with the information related to the hardware secure module, and checks whether the secure software is falsification based on a result of the comparison." For the above-discussed reason, the Examiner does not appear to have established a priori case of anticipation. For this reason it is requested that the rejection be withdrawn.

As such the claimed invention solves problems existing in Ebrahim as the tamper resistant module structure enables prevention (physically and logically) of an unauthorized access. There is no such teaching in Ebrahim.

Therefore, Ebrahim does not disclose or suggest each and every element of the Applicants' independent claims. Therefore, since Ebrahim does not disclose the features recited in the independent claims, as stated above, it is respectfully submitted that the independent claims patentably distinguishes over Ebrahim, and withdrawal of the §102(b) rejection is earnestly and respectfully solicited.

Claims depending from the independent claims include all of the features of that claim plus additional features which are not disclosed by Ebrahim. For at least the above-mentioned reasons, claims depending from the independent claims are patentably distinguishable over Ebrahim. The dependent claims are also independently patentable.

For example, as recited in claim 18, "the secret information is stored in a controlled memory space" and the controlled memory space is such that "a correct information is read out from the memory space at a first time and an incorrect information is read out at a second time". Ebrahim does not teach or suggest these features of claim 18.

Therefore, withdrawal of the rejection is respectfully requested.

CLAIM REJECTIONS UNDER 35 USC § 103:

In the Office Action the Examiner rejected claims 13-18 and 33-38 under 35 U.S.C. §103(a) as being unpatentable over Ebrahim in light of U.S. Patent No. 5,022,077 (Bealkowski). The Applicants respectfully traverse the Examiner's rejections of the remaining claims.

As mentioned above, the independent claims patentably distinguish over Ebrahim. The above presented arguments with respect to the independent claims are incorporated herein to

address the rejection of dependent claims 13-18 and 33-38. For at least the same reasons, the dependent claims are also patentably distinguishable over Ebrahim.

Further, as Bealkowski merely discusses a protected region that has a BIOS image loaded into a memory and activated using the operating system to prevent access to the region, Bealkowski does not cure the deficiencies of Ebrahim regarding claims of the present application.

Even assuming arguendo that Bealkowski does disclose the features discussed by the Examiner, the Applicants respectfully submit that there is no motivation to combine the cited references. The Examiner stated that the combination of the references would be obvious in order to allow authorized system to boot-up BIOS image as taught in Bealkowski at col. 30-56.

The record, however, fails to provide the required evidence of a motivation for a person of ordinary skill in the art to perform such modification. While Bealkowski may provide a reason for using the boot-up BIOs image, Ebrahim fails to suggest why a person of ordinary skill in the art at the time of the invention would be motivated to incorporate the use such as discussed in Bealkowski.

Moreover, even if Ebrahim and Bealkowski were combined, the teachings thereof do not teach or suggest the invention of as claimed in claims 13-18 and 33-38.

Therefore, withdrawal of the rejection is respectfully requested.

CONCLUSION:

There being no further outstanding objections or rejections, it is submitted that the application is in condition for allowance. An early action to that effect is courteously solicited.

Finally, if there are any formal matters remaining after this response, the Examiner is requested to telephone the undersigned to attend to these matters. If there are any additional fees associated with filing of this Amendment, please charge the same to our Deposit Account No. 19-3935.

Respectfully submitted,

STAAS & HALSEY LLP

Date: 09/15/2010 By: Temnit Afework

1201 New York Avenue, N.W., 7th Floor
Washington, D.C. 20005
Telephone: (202) 434-1500 ** Facsimile: (202) 434-1501

Temnit Afework
Registration No. 58,202